International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Trapping Unauthorized Signals in Jammer

Meena Kudande[1], D. C. Mehetre[2]

Department of Computer Engineering, KJ's College of Engineering & M. R., Pune, India

Professor, Department of Computer Engineering, KJ's College of Engineering & M. R., Pune, India

Abstract: ***This paper presents a mechanism, called Authorized Jammer, which provide jamming capability that can trapped unauthorized wireless signals and at the same time access authorized communication. The jammer jams the wireless signals continuously by using secret keys, so that the jamming signals identify the signals come from unauthorized devices, and can access the signals by authorized devices with the secret keys. To achieve this jammer by developing new design circuit for trapping the signals. This paper assume authorized devices as mobile phones signals and other than that assume unauthorized devices.***

Keywords: Authorized Jammer, Public Key cryptography, Elliptic curve etc.

1. Introduction

In our day-to-day life most of the peoples depend on wireless communication systems in many aspects. The wireless medium is easy to access and open for everyone. Now a day using Wi-Fi and mobile phones it becomes ease of use. So this openness of wireless medium can become a big problem for security. It creates problem by attacks from malicious users like terrorism attacks.

For example, using wireless communication a common way to trigger explosive devices like roadside bombs, which were responsible for deaths of thousands of lives or illegal broadcasting? Illegal broadcasting can cause Network problem, e.g. those used by air traffic control and the emergency services.
Such communication can be secure using jammer devices called Authorized jammer. Jammer can disable unauthorized wireless communication but at the same time still allow authorized wireless devices to Communicate. For some author [8] [10] provided jammer that disable all communication by

Providing secrete key
After some initial studies of jammer [2] a deliberating jammer jamming, radio signals is the equivalent of an Internet denial of service attack. Spoofing legitimate users, denying service to legitimate nodes, or eavesdropping [3]. These attacks can focus on a whole network of nodes or on a single link in the network.

2. System Model

1) Jammer: jammer is electronic device that jams the signals within specific effective range. There are different types of jammer
   a. Mobile Jammer
   b. Radar Jammer
   c. TV Remote Jammer
   d. Bluetooth Jammer

Deliberate jamming, which for radio signals is the equivalent of an internet denial of service attack [2]. So these jammers are already available but not have the capability to jams only unauthorized signals and attach to the CCTV camera. This paper presents jammer which aims to jam only unauthorized signals and attach to the CCTV camera.

Threat Model: here assume that unauthorized devices as potential adversaries. The objective of unauthorized devices is to understand the proposed scheme so that they cannot communicate to the other devices. They may analyze the jamming signals and attempt to use the result of analysis to remove the jamming signals with signal processing techniques ([8] [9]). They may also employ anti-jamming communication techniques such as Direct Sequence Spread Spectrum (DSSS), Frequency Hopping Spread Spectrum (FHSS), and their variations ([4] [5] [6])

Jammer Design:

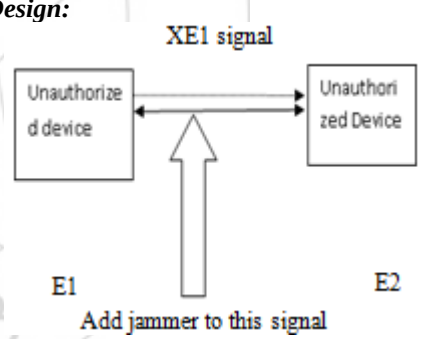

Figure 1: Trapping Unauthorized signals using jammer

When unauthorized device E1 transmits signals E1 to another unauthorized device E2, the jammer add its own signal i.e. XJ and received by E2. The jamming signals from XJ can effectively distort the signals XE1 at E2. As a result, the wireless communication between unauthorized devices E1 and E2 is disabled.

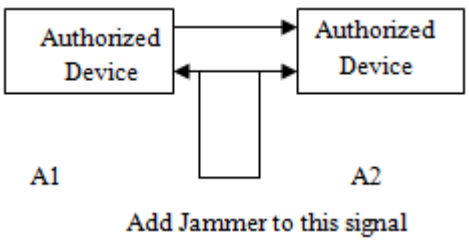

Figure 2: Access authorized signals using jammer

When A1 transmits signals XA1 to A2, the jamming signals XJ will add to this signal and received at A2. Since A2

shares the same secrete key k with XJ. It can generate the same jamming signals XJ using K. so that it removes the portion of XJ & get the original signal of XA1 at A2. This way authorized devices can access the signals using public shared secrete key.

3. Generation of Jamming Signals

Every jammer uses a shared, unique secrete key to generate its jamming signals. Our jammer and authorized devices shares a set of same secrete key. Hence here use of Diffie-Hellman key agreement algorithm.

Diffie-Hellman Key Agreement:
In the Diffie-Hellmen protocol two devices create a symmetric session key. Before establishing a symmetric key, the two devices need to choose two numbers i.e. P for large prime number and g for generate the number (P-1). Here assume that authorized devices given one unique number and that number will be match to the jammer. When authorized device A send signal to the other authorized devices B then it sends encrypted key i.e. $R1=g^x \bmod p$

When this signal is trapped by jammer then jammer use its unique key and apply on this signal. If the key is matched then it sends signals to the destination.

Every devices given unique key say k. if device A send signal then it added its unique key.

Other device send encrypted key i.e. $R2= g^y \bmod p$. so here x & y are the separate unique key for each devices. Now the jammer matches these keys to the jammer key if it matches then it disables its function. If jammer disables its function then signals are easily passed to the other devices. If key is not match then jammer executes its function i.e. to jams the signals. so jammer has calculate the signals $k=g^{xy} \bmod p$.

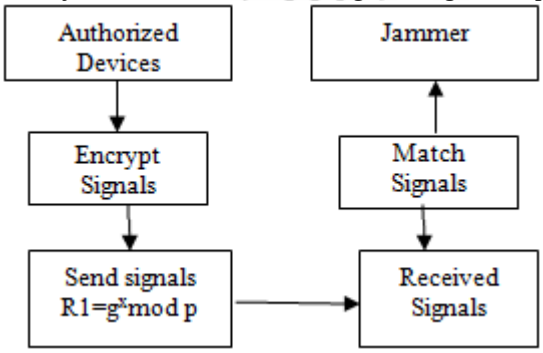

Figure 3: Transmitting signals from the authorized device to Jammer.

Example:
Here assume that x=3, p=27, g=2
Now $R1=g^x \bmod p$

$R1=2^3 \bmod 27$

R1=26
Now calculate $R2=g^y \bmod p$
Here y=2, p and g values are same.
$R2=2^2 \bmod 27$
R2=4 mod 27
R2=13.
Now calculate K1 by using R2 key.
$K1= (R2)^x \bmod p$
$K1= 13^3 \bmod 27$
K1=10
Then calculate $K2= (R1)^y \bmod p$
$K2=26^2 \bmod 27$
K2=10.
So here K1 and K2 both values are same. Means these are the authorized signals and communicates very securely. So jammer match this unique key and identify the device is authorized or not.

Analog of Diffie-Hellman Key exchange:
A key exchange between users A and B can be accomplished as follows
1. A select an integer n_A less than n. This is A's private key. A then generates a public key
$P_A = n_A * G$; the public key is a point in $E_q(a,b)$.
2. B similarly selects a private key n_B and computes a public key P_B.
3. A generates the secrete key $K=n_A*P_B$.
B generates the secrete key $K=n_B * P_A$.
The two calculations in step 3 produce the same result because
$N_A*P_B = n_A *(n_B*G)= n_B *(n_A *G)$
$= n_B * P_A$.

Elliptic curve encryption and decryption

For an encryption/decryption, system requires a point G and an elliptic group $E_q(a,b)$ as parameters. Each user A selects a private key n_A and generates a public key $P_{A=}n_A*G$. To encrypt and send message P_m to user B, A chooses a random positive integer K and produces the ciphertext C_m.
$C_m=\{KG,P_m+KP_B\}$
TO encrypt the ciphertext, B multiplies the first point in the pair by B's secrete key
$P_m+KP_B- n_B(KG)$
$=P_m + K(n_BG) - n_B(KG)$
$=P_m$

4. Conclusion

This paper presents the jammer that trapped unauthorized signals using public key cryptography. Here using a Diffie-Hellman Key agreement algorithm is used for key exchange. Authorized devices and jammer can exchange the key and identify the authorized devices. Whereas unauthorized devices do not exchange the key or wrong key exchange algorithms are given. So it identifies the signals which come from authorized or unauthorized devices. In this paper the future works include the robustness of jammer, attacks on different waves, capability against unauthorized devices etc.

References

[1] GNU Radio - The GNU Software Radio. http://gnuradio.org/ redmine/projects/gnuradio/wiki.
[2] H. Meyr, M. Moeneclaey, and S.A. Fechtel. *Digital communication receivers : synchronization, channel estimation, and signal processing*. John Wiley & Sons, 1998.

[3] H. Chan, A. Perrig, and D. Song. Random key predistribution schemes for sensor networks. In *IEEE Symposium on Security and Privacy*, 2003.
[4] D. Liu, P. Ning, and R. Li. Establishing pairwise keys in distributed sensor networks. *ACM Transactions on Information and System Security*, 2005.
[5] R. Poisel. *Modern Communications Jamming Principles and Techniques*. Artech House Publishers, 2006.
[6] J.G. Proakis and M. Salehi. *Digital communications*.McGraw-hill, 2008.
[7] A. Liu, P. Ning, H. Dai, and Y. Liu. USD-FH: Jammingresistant wireless communication using frequency hopping with uncoordinated seed disclosure. In *MASS*, 2010.
[8] B. DeBruhl and P. Tague. Digital filter design for jamming mitigation in 802.15.4 communication. In *ICCCN*, 2011.
[9] R.G. Lyons. *Understanding digital signal processing*. Prentice Hall, 2011.
[10] S. Sankararaman, K. Abu-Affash, A. Efrat, S. D. Eriksson-Bique, V. Polishchuk, S.Ramasubramanian, and M. Segal.Optimization schemes for protective jamming. In *MobiHoc*,2012.